Defense Information Systems Agency

A Combat Support Agency

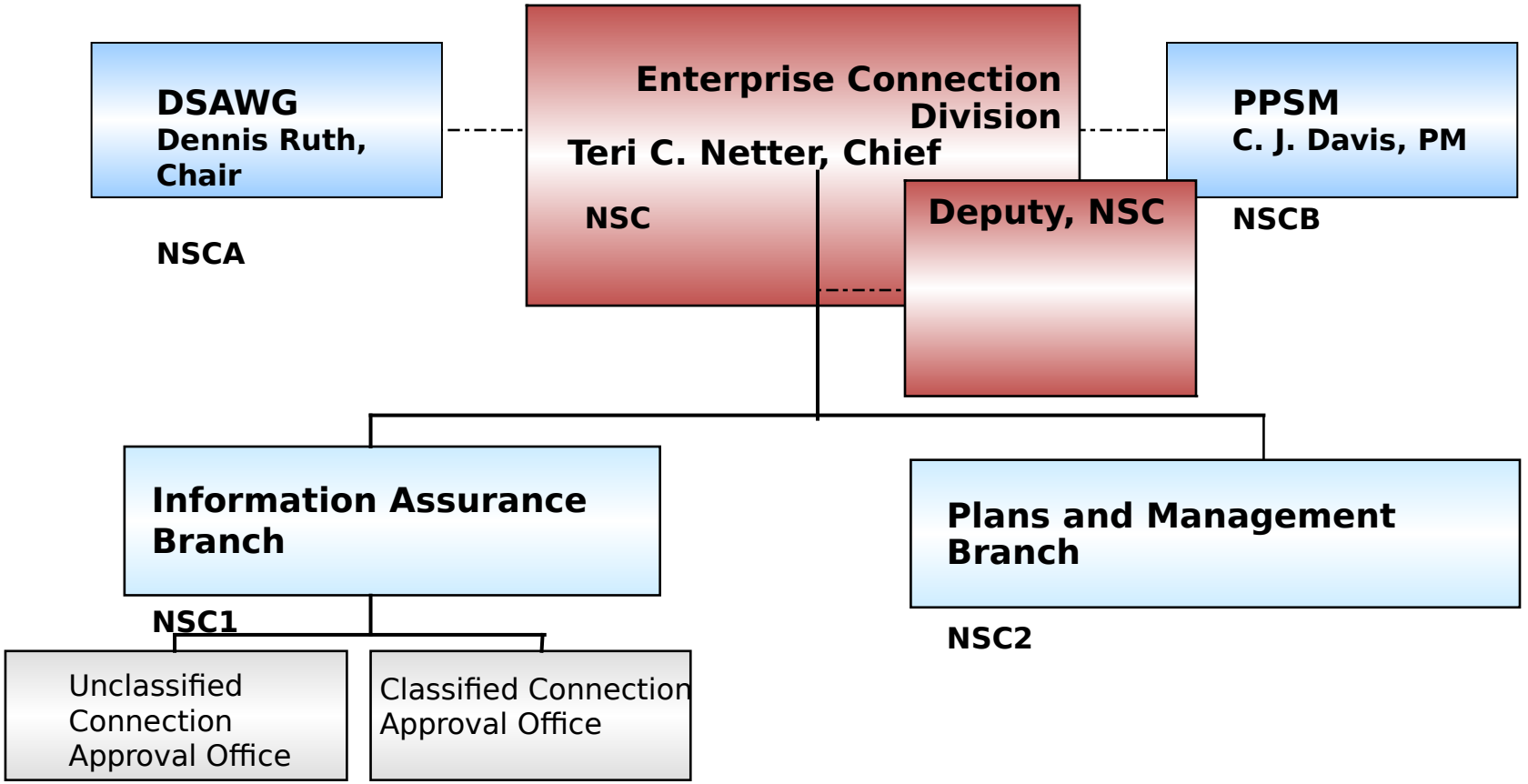
Ports, Protocols, and Services Management (PPSM)

15 - 19 August 2011

UNCLASSIFIED

DISA
A Combat Support Agency

Enterprise Connection Division



DISA
A Combat Support Agency

What is PPSM ?

Creates fundamental, definitive, but agile standards for controlling and regulating the use of IP protocols and data services based on vulnerability assessments, functional capabilities, and standardized implementation strategies that promote network security and interoperability across the Enterprise Networks.

PPSM provides support to:

- Acquisition, Design, Development, and Configuration
- Certification and Accreditation (C&A)
- Enterprise, Organization, and System DAAs
- GIG Connectivity (FSO/CAO/DSAWG/DISN PAA)
- Cybercom / NetOps / Perimeter defense
- Firewall Administrators

Best known use – to configure network security devices (e.g. routers, firewalls, and IDS/IPS)

DISA
A Combat Support Agency

Value of PPSM

- Researches and compiles multiple Information Assurance (IA) data sources to create unique assessment results that identify vulnerability, capability, and functionality.
- Promotes reciprocity and interoperability across and between DoD networks and Mission Partners.
- Provides a forum for CC/S/A vetting.
- Disseminates guidance for the regulation and enforcement of Network and Perimeter Defense activities.

Fosters the "building in" of security from the beginning of an application's lifecycle.

DISA
A Combat Support Agency

Potential Impact

- Certification & Accreditation (C&A) package
- Hosting/Fielding Systems in the Defense Enterprise Computing Centers (DECCs)
- May not be allowed to connect to GIG
- Traffic being Blocked by Destination Firewalls

Open and unnecessary IP protocols, data services and associated ports increase the risk of data compromise and system unavailability

DISA
A Combat Support Agency

Current PPSM Process

- **PPSM Registry: https://pnp.cert.smil.mil**
- **Commence assessment process**
- **Technical Advisory Group (TAG)**
- **CCB Votes on Vulnerability Assessments (VA)**
- **Products published on IASE and DKO websites (high/low)**

Information Assurance Support Environment – IASE

NIPRNet - http://iase.disa.mil/ports/index.html
SIPRNet - http://iase.disa.smil.mil/ports/index.html

Army Knowledge Online/Defense Knowledge Online - AKO/DKO

NIPRNet - https://www.us.army.mil/suite/page/396114
SIPRNet - http://www.us.army.smil.mil/suite/page/13648

DISA
A Combat Support Agency

Way Ahead

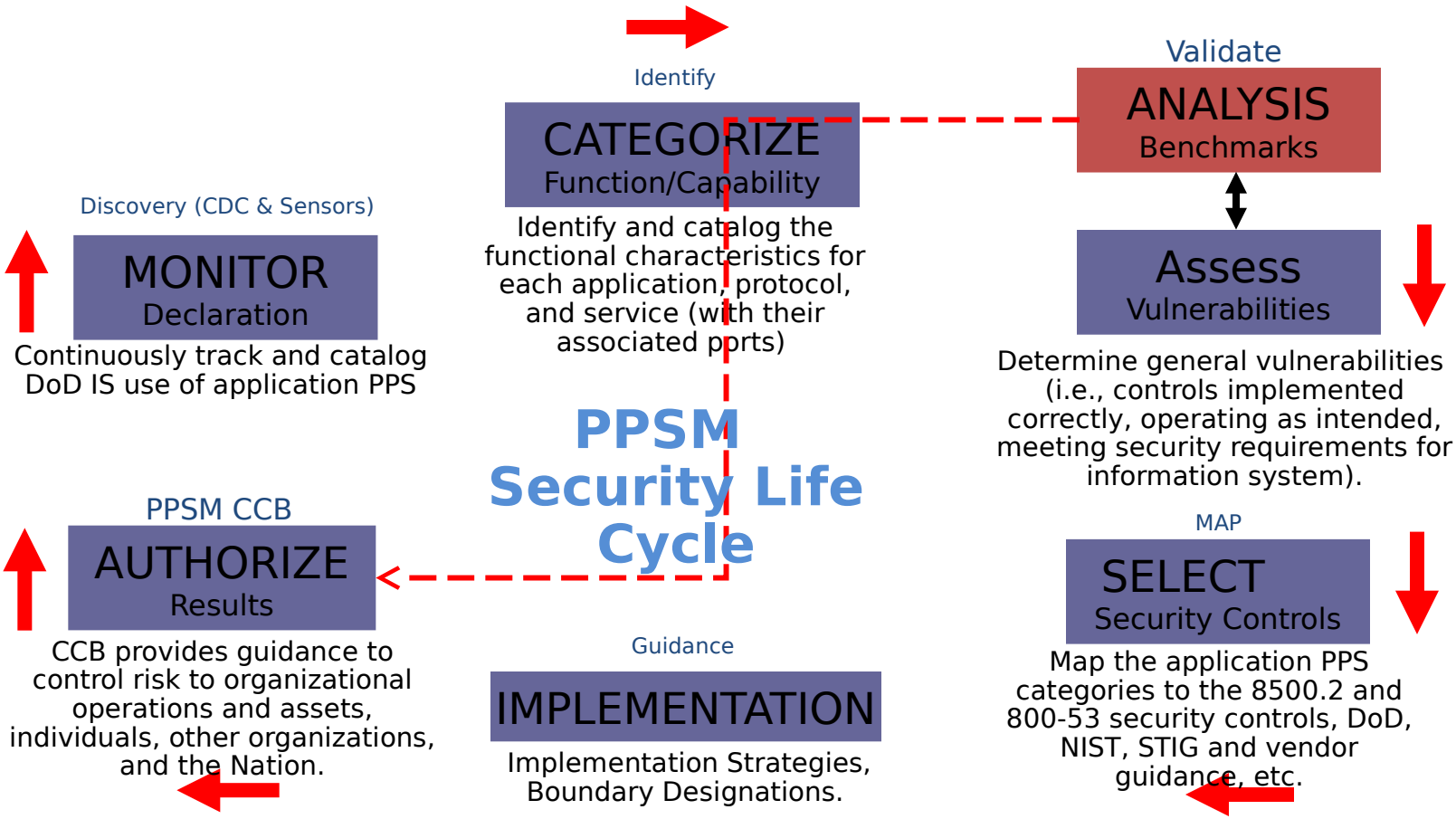
- Introduce new paradigm by re-writing DoDI 8551.1.
  - Operationalize PPSM Standards and Products.
- Automate situational awareness feeds to NetOPS/Cybercom.
- Supplement other repositories with PPSM assessment results.
- Ability to access the PPSM Standards and Products via the NIPRNet.

Restructuring for the Continuous Monitoring and Analysis of information systems

DISA
A Combat Support Agency

PPSM Risk Management Framework

Continuous Monitoring


Identify
CATEGORIZE
Function/Capability
Identify and catalog the functional characteristics for each application, protocol, and service (with their associated ports)
Validate
ANALYSIS
Benchmarks
Assess
Vulnerabilities
Determine general vulnerabilities (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).
MAP
SELECT
Security Controls
Map the application PPS categories to the 8500.2 and 800-53 security controls, DoD, NIST, STIG and vendor guidance, etc.
Guidance
IMPLEMENTATION
Implementation Strategies, Boundary Designations.
PPSM CCB
AUTHORIZE
Results
CCB provides guidance to control risk to organizational operations and assets, individuals, other organizations, and the Nation.
Discovery (CDC & Sensors)
MONITOR
Declaration
Continuously track and catalog DoD IS use of application PPS
PPSM Security Life Cycle

DISA

A Combat Support Agency

PPSM

“ Committed to Protecting Data End-to-End ”

Questions?

UNCLASSIFIED